UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/584,194	05/25/2007	Takehiro Ohkoshi	2565-0297PUS1	1262

2292 7590 04/03/2009

BIRCH STEWART KOLASCH & BIRCH
PO BOX 747
FALLS CHURCH, VA 22040-0747

EXAMINER	
ABRISHAMKAR, KAVEH	
ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
04/03/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

mailroom@bskb.com

Office Action Summary	Application No.	Applicant(s)	
	10/584,194	OHKOSHI ET AL.	
	Examiner	Art Unit	
	KAVEH ABRISHAMKAR	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 December 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to the amendment filed on December 19, 2008. Claims 1-10 were originally pending consideration. No claims were amended or added by virtue of the received amendment.

2. Claims 1-10 are currently pending consideration.

Response to Arguments

Applicant's arguments filed 12/19/2008 have been fully considered but they are not persuasive for the following reasons:

Regarding claim 1, the Applicant argues that the Cited Prior Art (CPA), Edgett et al. (U.S. Patent Pub. No. 2004/0034771), does not disclose receiving a prescribed algorithm identifier and a prescribed encryption key identifier, selected from among the at least one algorithm identifier and the at least one encryption key identifier transmitted by the transmitting unit. This argument is not found persuasive. The CPA discloses updating the algorithm, by changing the key pair (paragraph 0057). In doing this, the CPA discloses providing a ***key index*** (encryption key identifier) and an ***algorithm identifier*** (paragraph 0058). The CPA discloses an index to identify the key and an algorithm to identify the algorithm (paragraph 0058). Therefore, it is asserted that the CPA does teach receiving a prescribed algorithm identifier and a prescribed encryption key identifier, selected from among the at least one algorithm identifier and the at least one encryption key identifier transmitted by the transmitting unit.

Therefore, the rejection for the claims is respectfully maintained as given below.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-10 are rejected under 35 U.S.C. 102 (e) as being anticipated by Edgett et al. (U.S. Patent Pub. No. US 2004/0034771)

Regarding claim 1, Edgett discloses:

An authenticated device comprising:

a memory unit to store at least one algorithm identifier and at least one encryption key identifier (paragraph 0058: *key pair, key index, and algorithm identifier all stored in private key database*);

a transmitting unit to transmit the at least one algorithm identifier and the at least one encryption key identifier stored by the memory unit to an authenticating device (paragraph 0057: *key index and algorithm are sent to the authentication server*);

a receiving unit to receive from the authenticating device a prescribed algorithm identifier and a prescribed encryption key identifier, selected from among the at least one algorithm identifier and the at least one encryption key identifier transmitted by the transmitting unit (paragraph 0059: *the updated algorithm and key are sent back to the dialer to be used for subsequent connections*); and

an authentication processing unit to perform an authentication process with the authenticating device, based on the prescribed algorithm identifier and the prescribed encryption key identifier received by the receiving unit (paragraph 0058: *password is decrypted and authenticated*).

Claim 2 is rejected as applied above in rejecting claim 1. Furthermore, Edgett discloses:

The authenticated device of claim 1,

wherein the memory unit stores at least one algorithm identifier and at least one encryption key identifier in such a manner that one algorithm identifier and one encryption key identifier are paired as one profile (paragraph 0058: *key pair, key index, and algorithm identifier all stored in private key database*);

wherein the transmitting unit transmits, to the authenticating device, the at least one algorithm identifier and the at least one encryption key identifier stored by the memory unit in such a manner that one algorithm identifier and one encryption key identifier are paired as one profile (paragraph 0057: *key index and algorithm are sent to the authentication server*);

wherein the receiving unit receives, from the authenticating device, the prescribed algorithm identifier and the prescribed encryption key identifier paired as a prescribed profile, among the at least one algorithm identifier and the at least one encryption key identifier transmitted by the transmitting unit (paragraph 0059: *the updated algorithm and key are sent back to the dialer to be used for subsequent connections*); and

wherein the authentication processing unit performs the authentication process with the authenticating device, based on the prescribed algorithm identifier and the prescribed encryption key identifier paired as the prescribed profile received by the receiving unit (paragraph 0058: *password is decrypted and authenticated*).

Claim 3 is rejected as applied above in rejecting claim 2. Furthermore, Edgett discloses:

The authenticated device of claim 2,

wherein the memory unit further stores a version identifier to identify a version indicating a set in such a manner that one set is formed from at least one algorithm corresponding to the at least one algorithm identifier stored (paragraph 0055: *version number is stored which contains a key index and an algorithm identifier*);

wherein the transmitting unit transmits the version identifier stored by the memory unit to the authenticating device (paragraph 0057: *key index and algorithm are sent to the authentication server*);

wherein the receiving unit receives, from the authenticating device, the prescribed algorithm identifier corresponding to a prescribed algorithm among the at least one algorithm forming the set indicated by the version identified by the version identifier transmitted from the transmitting unit (paragraph 0059: *the updated algorithm and key are sent back to the dialer to be used for subsequent connections*); and

wherein the authentication processing unit performs the authentication process with the authenticating device, based on the prescribed algorithm identifier received by the receiving unit and on a prescribed encryption key identifier paired with the prescribed algorithm identifier (paragraph 0058: *password is decrypted and authenticated*).

Regarding claim 4, Edgett discloses:

An authenticating device comprising:

a memory unit to store at least one algorithm identifier and at least one encryption key identifier; a receiving unit to receive at least one algorithm identifier and at least one encryption key identifier from an authenticated device (paragraph 0058: *key pair, key index, and algorithm identifier all stored in private key database*);

a selecting unit to select a prescribed algorithm identifier and a prescribed encryption key identifier to be stored by the memory unit from among the at least one algorithm identifier and the at least one encryption key identifier received by the receiving unit (paragraph 0057: *key index and algorithm are stored in a private key database*), when the at least one algorithm identifier and the at least one encryption key

identifier stored by the memory unit exist among the at least one algorithm identifier and the at least one encryption key identifier received by the receiving unit (paragraph 0057: *key index and algorithm are stored in a private key database*);

a transmitting unit to transmit the prescribed algorithm identifier and the prescribed encryption key identifier selected by the selecting unit to the authenticated device (paragraph 0059: *the updated algorithm and key are sent back to the dialer to be used for subsequent connections*); and

an authentication processing unit to perform an authentication process with the authenticated device, based on the prescribed algorithm identifier and the prescribed encryption key identifier transmitted by the transmitting unit (paragraph 0058: *password is decrypted and authenticated*).

Claim 5 is rejected as applied above in rejecting claim 4. Furthermore, Edgett discloses:

The authenticating device of claim 4,

wherein the memory unit stores at least one profile identifier to identify at least one profile, whereby one algorithm identifier among the at least one algorithm identifier and one encryption key identifier among the at least one encryption key identifier are paired (paragraph 0058: *key pair, key index, and algorithm identifier all stored in private key database*);

wherein the receiving unit further receives at least one profile identifier from the authenticated device (paragraph 0059: *the updated algorithm and key are sent back to the dialer to be used for subsequent connections*);

wherein the selecting unit selects a prescribed profile identifier to be stored by the memory unit from among the at least one profile identifier received by the receiving unit, when the at least one profile identifier stored by the memory unit exists among the at least one profile identifier received by the receiving unit (paragraph 0059: *if an update is required, downloading the new algorithm and key*);

wherein the transmitting unit transmits the prescribed profile identifier selected by the selecting unit to the authenticated device (paragraph 0059: *the updated algorithm and key are sent back to the dialer to be used for subsequent connections*); and

wherein the authentication processing unit performs the authentication process with the authenticated device, based on the prescribed algorithm identifier and the prescribed encryption key identifier paired by a prescribed profile identified by the prescribed profile identifier transmitted by the transmitting unit (paragraph 0058: *password is decrypted and authenticated*).

Claim 6 is rejected as applied above in rejecting claim 5. Furthermore, Edgett discloses:

The authenticating device of claim 5,

wherein the memory unit further stores a version identifier to identify a version of a set in such a manner that one set is formed from at least one algorithm corresponding

to the at least one algorithm identifier stored (paragraph 0055: *version number is stored which contains a key index and an algorithm identifier*);

wherein the receiving unit further receives a prescribed version identifier from the authenticated device (paragraph 0055: *version number is stored which contains a key index and an algorithm identifier and the update server supplies the version number*);

wherein the selecting unit selects the prescribed algorithm identifier corresponding to one algorithm in the set indicated by the version identified by the prescribed version identifier received by the receiving unit (paragraph 0059: *if an update is required, downloading the new algorithm and key*);

wherein the transmitting unit transmits the prescribed algorithm identifier selected by the selecting unit to the authenticated device profile (paragraph 0057: *key index and algorithm are sent to the authentication server*); and

wherein the authentication processing unit performs the authentication process with the authenticated device, based on the prescribed algorithm identifier transmitted by the transmitting unit and on a prescribed encryption key identifier paired with the prescribed algorithm identifier (paragraph 0058: *password is decrypted and authenticated*).

Regarding claim 7, Edgett discloses:

An authenticating method comprising:

a first transmitting step to transmit, from an authenticated device storing a plurality of algorithm identifiers and a plurality of encryption key identifiers, to an

authenticating device, the plurality of algorithm identifiers and the plurality of encryption key identifiers stored (paragraph 0058: *key pair, key index, and algorithm identifier all stored in private key database*);

a first receiving step to receive the plurality of algorithm identifiers and the plurality of encryption key identifiers transmitted from the authenticated device by the first transmitting step, at the authenticating device storing at least one algorithm identifier and at least one encryption key identifier (paragraph 0055: *version number is stored which contains a key index and an algorithm identifier and the update server supplies the version number*);

a selecting step to select, at the authenticating device, a prescribed algorithm identifier and a prescribed encryption key identifier to be stored by the authenticating device from among the plurality of algorithm identifiers and the plurality of encryption key identifiers received by the receiving step, when the at least one algorithm identifier and the at least one encryption key identifier stored by the authenticating device exist among the plurality of algorithm identifiers and the plurality of encryption key identifiers received by the first receiving step (paragraph 0059: *if an update is required, downloading the new algorithm and key*);

a second transmitting step to transmit the prescribed algorithm identifier and the prescribed encryption key identifier selected by the selecting step, from the authenticating device to the authenticated device paragraph 0057: *key index and algorithm are sent to the authentication server*);

a second receiving step to receive the prescribed algorithm identifier and the prescribed encryption key identifier transmitted by the second transmitting step, from the authenticating device, at the authenticated device (paragraph 0059: *the updated algorithm and key are sent back to the dialer to be used for subsequent connections*); and

an authentication processing step to perform an authentication process between the authenticating device and the authenticated device, based on the prescribed algorithm identifier and the prescribed encryption key identifier received by the second receiving step (paragraph 0058: *password is decrypted and authenticated*).

Regarding claim 8, Edgett discloses:

An authenticating method comprising:

a first transmitting step to transmit, from an authenticated device storing at least one algorithm identifier and at least one encryption key identifier, to an authenticating device, the at least one algorithm identifier and the at least one encryption key identifier stored (paragraph 0058: *key pair, key index, and algorithm identifier all stored in private key database*);

a first receiving step to receive the at least one algorithm identifier and the at least one encryption key identifier transmitted from the authenticated device by the first transmitting step, at the authenticating device storing a plurality of algorithm identifiers and a plurality of encryption key identifiers (paragraph 0055: *version number is stored*

which contains a key index and an algorithm identifier and the update server supplies the version number);

a selecting step to select, at the authenticating device, a prescribed algorithm identifier and a prescribed encryption key identifier to be stored by the authenticating device from among the at least one algorithm identifier and the at least one encryption key identifier received by the receiving step, when at least one of the plurality of algorithm identifiers and at least one of the plurality of encryption key identifiers stored by the authenticating device exist among the at least one algorithm identifier and the at least one encryption key identifier received by the first receiving step (paragraph 0059: *if an update is required, downloading the new algorithm and key*);

a second transmitting step to transmit the prescribed algorithm identifier and the prescribed encryption key identifier selected by the selecting step, from the authenticating device to the authenticated device (paragraph 0059: *the updated algorithm and key are sent back to the dialer to be used for subsequent connections*);

a second receiving step to receive the prescribed algorithm identifier and the prescribed encryption key identifier transmitted by the second transmitting step, from the authenticating device, at the authenticated device (paragraph 0059: *the updated algorithm and key are sent back to the dialer to be used for subsequent connections*); and

an authentication processing step to perform an authentication process between the authenticating device and the authenticated device, based on the prescribed

algorithm identifier and the prescribed encryption key identifier received by the second receiving step (paragraph 0058: *password is decrypted and authenticated*).

Regarding claim 9, Edgett discloses:

An authenticating method comprising:

transmitting, from an authenticated device storing a plurality of algorithm identifiers and a plurality of encryption key identifiers, to an authenticating device, the plurality of algorithm identifiers and the plurality of encryption key identifiers stored (paragraph 0058: *key pair, key index, and algorithm identifier all stored in private key database*);

receiving the plurality of algorithm identifiers and the plurality of encryption key identifiers transmitted from the authenticated device, at the authenticating device storing at least one algorithm identifier and at least one encryption key identifier (paragraph 0059: *the updated algorithm and key are sent back to the dialer to be used for subsequent connections*);

selecting, at the authenticating device, a prescribed algorithm identifier and a prescribed encryption key identifier to be stored by the authenticating device from among the plurality of algorithm identifiers and the plurality of encryption key identifiers received, when the at least one algorithm identifier and the at least one encryption key identifier stored by the authenticating device exist among the plurality of algorithm identifiers and the plurality of encryption key identifiers received (paragraph 0059: *if an update is required, downloading the new algorithm and key*);

transmitting the prescribed algorithm identifier and the prescribed encryption key identifier selected, from the authenticating device to the authenticated device device (paragraph 0059: *the updated algorithm and key are sent back to the dialer to be used for subsequent connections*);

receiving the prescribed algorithm identifier and the prescribed encryption key identifier transmitted from the authenticating device, at the authenticated device device (paragraph 0059: *the updated algorithm and key are sent back to the dialer to be used for subsequent connections*); and

performing an authentication process between the authenticating device and the authenticated device, based on the prescribed algorithm identifier and the prescribed encryption key identifier received (paragraph 0058: *password is decrypted and authenticated*).

Regarding claim 10, Edgett discloses:

An authenticating method comprising:

transmitting, from an authenticated device storing at least one algorithm identifier and at least one encryption key identifier, to an authenticating device, the at least one algorithm identifier and the at least one encryption key identifier stored (paragraph 0058: *key pair, key index, and algorithm identifier all stored in private key database*);

receiving the at least one algorithm identifier and the at least one encryption key identifier transmitted from the authenticated device, at the authenticating device storing a plurality of algorithm identifiers and a plurality of encryption key identifiers (paragraph

0055: *version number is stored which contains a key index and an algorithm identifier and the update server supplies the version number*);

selecting, at the authenticating device, a prescribed algorithm identifier and a prescribed encryption key identifier to be stored by the authenticating device from among the at least one algorithm identifier and the at least one encryption key identifier received, when at least one of the plurality of algorithm identifiers and at least one of the plurality of encryption key identifiers stored by the authenticating device exist among the at least one algorithm identifier and the at least one encryption key identifier received (paragraph 0059: *if an update is required, downloading the new algorithm and key*);

transmitting the prescribed algorithm identifier and the prescribed encryption key identifier selected, from the authenticating device to the authenticated device device (paragraph 0059: *the updated algorithm and key are sent back to the dialer to be used for subsequent connections*);

receiving the prescribed algorithm identifier and the prescribed encryption key identifier transmitted from the authenticating device, at the authenticated device device (paragraph 0059: *the updated algorithm and key are sent back to the dialer to be used for subsequent connections*); and

performing an authentication process between the authenticating device and the authenticated device, based on the prescribed algorithm identifier and the prescribed encryption key identifier received (paragraph 0058: *password is decrypted and authenticated*).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to KAVEH ABRISHAMKAR whose telephone number is (571)272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Kaveh Abrishamkar/
Primary Examiner, Art Unit 2431

/K. A./
03/28/2009
Primary Examiner, Art Unit 2431